UNIT I - INTRODUCTION

Ethical Hacking Overview – Role of Security and Penetration Testers. – Penetration –Testing Methodologies - Laws of the Land - Overview of TCP/IP - The Application Layer - The Transport Layer – The Internet Layer – IP Addressing. - Network and Computer Attacks – Malware – Protecting Against Malware Attacks. – Intruder Attacks - Addressing Physical Security

1.1 Ethical Hacking Overview

Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

Hacking is usually legal as long as it is being done to find weaknesses in a computer or network system for testing purpose. This sort of hacking is what we call **Ethical Hacking**.

Definition: Ethical hacking is an authorized practice of detecting vulnerabilities in an application, system, or organization's infrastructure and bypassing system security to identify potential data breaches and threats in a network.

Ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy. They collect and analyze the information to figure out ways to strengthen the security of the system/network/applications. By doing so, they can improve the security footprint so that it can better withstand attacks or divert them.

Ethical hackers are hired by organizations to look into the vulnerabilities of their systems and networks and develop solutions to prevent data breaches. Consider it a high-tech permutation of the old saying "It takes a thief to catch a thief."

Types of Hacking:

- **Website Hacking** − Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.
- **Network Hacking** − Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.
- **Email Hacking** − It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.

- **Ethical Hacking** − Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.
- **Password Hacking** − This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
- **Computer Hacking** − This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

Advantages of Hacking:

Hacking is quite useful in the following scenarios −

- To recover lost information, especially in case you lost your password.
- To perform penetration testing to strengthen computer and network security.
- To put adequate preventative measures in place to prevent security breaches.
- To have a computer system that prevents malicious hackers from gaining access.

Disadvantages of Hacking:

Hacking is quite dangerous if it is done with harmful intent. It can cause −

- Massive security breach.
- Unauthorized system access on private information.
- Privacy violation.
- Hampering system operation.
- Denial of service attacks.
- Malicious attack on the system.

Types of Hackers:

Hackers can be classified into 3 categories -

1. White Hat Hackers
2. Black Hat Hackers
3. Grey Hat Hackers

1.White Hat Hackers:

White hat hackers are the one who is **authorized or the certified hackers** who work for the government and organizations by performing penetration testing and identifying loopholes in their cybersecurity. They also ensure the protection from the malicious cyber crimes. They work under the rules and regulations provided by the government, that's why they are called **Ethical hackers or Cybersecurity experts.**

2.Black Hat Hackers:

They are often called **Crackers.** Black Hat Hackers can gain the unauthorized access of your system and destroy your vital data. The method of attacking they use common hacking practices they have learned earlier. They are considered to be as criminals and can be easily identified because of their malicious actions.

3.Gray Hat Hackers:

Gray hat hackers fall somewhere in the category between white hat and black hat hackers. They can hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system. Gray hat hacking is sometimes acted legally and sometimes not.

Difference between Hacking and Ethical Hacking:

Hacking	Ethical Hacking
Steal valuable information of company and individual for illegal activity.	Hack system to reduce vulnerabilities of company's system.
Illegal practice and considered a crime.	Legal practice authorized by the company or individual.
They are called as black hat hackers.	They are called as white hat hackers.
They work for themselves for dirty money.	They work with different government agencies and big tech companies.
Try to access the restricted network through illegal practices and reduce the security of data.	They create firewalls and security protocols.

Similarities between hacking and ethical hacking:

- Whether it be a white hat hacker, black hat or grey hat hackers, they use the same tools for hacking.
- All the hackers have in-depth and strong knowledge of networks, OS and computer fundamentals.

1.2 Role of Security and Penetration Testers

A **hacker** accesses a computer system or network without the authorization of the system's owner. By doing so, a hacker is breaking the law and can go to prison. Those who break into systems to steal or destroy data are often referred to as crackers; hackers might simply want to prove how vulnerable a system is by accessing the computer or network without destroying any data.

An **ethical hacker** is a person who performs most of the same activities a hacker does but with the owner or company's permission. Ethical hackers are usually contracted to perform penetration tests or security tests. Companies realize that intruders might attempt to access their network resources, and are willing to pay for someone to discover these vulnerabilities first. Companies would rather pay a "good hacker" to discover problems in their current network configuration than have a "bad hacker" discover these vulnerabilities. Bad hackers spend many hours scanning systems over the Internet, looking for openings or vulnerable systems.

Some hackers are skilful computer experts, but others are younger, inexperienced people who experienced hackers refer to as **script kiddies or packet monkeys**. These derogatory terms refer to people who copy code from knowledgeable programmers instead of creating the code themselves. Many experienced penetration testers can write computer programs or scripts in Perl (Practical Extraction and Report Language) or the C language to carry out network attacks. (A script is a set of instructions that run in sequence to perform tasks on a computer system.)

What is a Penetration Test?

A penetration test is a subclass of ethical hacking; it comprises a set of methods and procedures that aim at testing/protecting an organization's security. A penetration test, also known as a "**pen test**," is a simulated cyber attack on a computer system, network, or web application.

Definition: The purpose of a penetration test is to identify vulnerabilities in the system that an attacker could exploit, and to evaluate the effectiveness of the system's security controls. Pen testers use the same tools, techniques, and processes as attackers to find and demonstrate the business impacts of weaknesses in system.

In a **penetration test**, an ethical hacker attempts to break into a company's network to find the weakest link in the network or a network system and report the findings to the company.
In a **security test**, testers do more than attempt to break in; they also analyze a company's security policy and procedures and report any vulnerabilities to management and offering solutions for securing or protecting the network.

Penetration testers and security testers usually have a laptop computer configured with multiple OSs and hacking tools. This collection of tools for conducting vulnerability assessments and attacks is sometimes referred to as a "**tiger box**".

Why pen testing required?

- It helps to find weak areas where an intruder can attack to gain access to the computer's features and data.

- It supports to avoid the black hat attack and protects the original data.

When to perform pen testing?

Pen Testing is an essential feature that needs to be performed regularly for securing the functioning of a system.

It should be performed whenever,

- the system is updated or installed new software
- new end user program / policy set up
- new network infrastructure added
- security system discovers new threats by attackers
- the office is relocated.

Role of Penetration Testers:

- Perform vulnerability, attack, and penetration assessments in Internet, intranet, and wireless environments.
- Perform discovery and scanning for open ports and services.
- Apply appropriate exploits to gain access and expand access as necessary.
- Participate in activities involving application penetration testing and application source code review.
- Interact with the client as required throughout the engagement.
- Produce reports documenting discoveries during the engagement.
- Debrief with the client at the conclusion of each engagement.
- Participate in research and provide recommendations for continuous improvement.
- Participate in knowledge sharing.

Responsibilities as a penetration tester, you'll need to:

- understand complex computer systems and technical cyber security terms
- work with clients to determine their requirements from the test, for example, the number and type of systems they would like testing
- plan and create penetration methods, scripts and tests
- carry out remote testing of a client's network or onsite testing of their infrastructure to expose weaknesses in security
- simulate security breaches to test a system's relative security

- create reports and recommendations from your findings, including the security issues uncovered and level of risk
- advise on methods to fix or lower security risks to systems
- present your findings, risks and conclusions to management and other relevant parties
- consider the impact your 'attack' will have on the business and its users
- understand how the flaws that you identify could affect a business, or business function, if they're not fixed.

Penetration tester tasks and responsibilities:

- Perform tests on applications, network devices, and cloud infrastructures
- Design and conduct simulated social engineering attacks
- Research and experiment with different types of attacks
- Develop methodologies for penetration testing
- Review code for security vulnerabilities
- Reverse engineer malware or spam
- Document security and compliance issues
- Automate common testing techniques to improve efficiency
- Write technical and executive reports
- Communicate findings to both technical staff and executive leadership
- Validate security improvements with additional testing

Benefits of Pen Testing:

1.Enhancement of the management system

- It provides detailed information about the security threats.
- It categorizes the degree of vulnerabilities and suggest which one is more vulnerable and which one is less.
- The user can easily and accurately manage the security system by allocating security resources accordingly.

2. Avoid Penalties / Fines

- Helps in keeping the major activities updated in one's organization.

3. Protection from financial damage

- Pen testing can protect the organization from financial damage because a simple breach of a security system may cause millions of dollars of damage.

4. Customer protection

- Pen testing can protect the organization from keeping the customers data intact and helps in avoiding financial and reputation damage.

1.3 Penetration –Testing Methodologies

Penetration testing can be defined as a legal and authorized attempt to locate and successfully exploit computer systems for the purpose of making those systems more secure. The process includes probing for vulnerabilities as well as providing proof of concept attacks to demonstrate the vulnerabilities are real. Proper penetration testing always ends with specific recommendations for addressing and fixing the issues that were discovered during the test. On the whole, this process is used to help secure computers and networks against future attacks. The general idea is to find security issues by using the same tools and techniques as an attacker. These findings can then be mitigated before a real hacker exploits them.

Ethical hackers who perform penetration tests use one of these models:

- White box penetration testing
- Black box penetration testing
- Grey box penetration testing

White Box Penetration Testing:

In this testing method attackers have developer-level knowledge about the system which also includes an assessment of source code, Ethical hackers have full access to the system more in-depth than black box testing. It is used to find out potential threats to the system due to bad programming, misconfigurations, or lack of any defensive measures.

For example, the company might print a network diagram showing all the company's routers, switches, firewalls, and intrusion detection systems (IDSs) or give the tester a floor plan detailing the location of computer systems and the OSs running on these systems (fig 1.1).

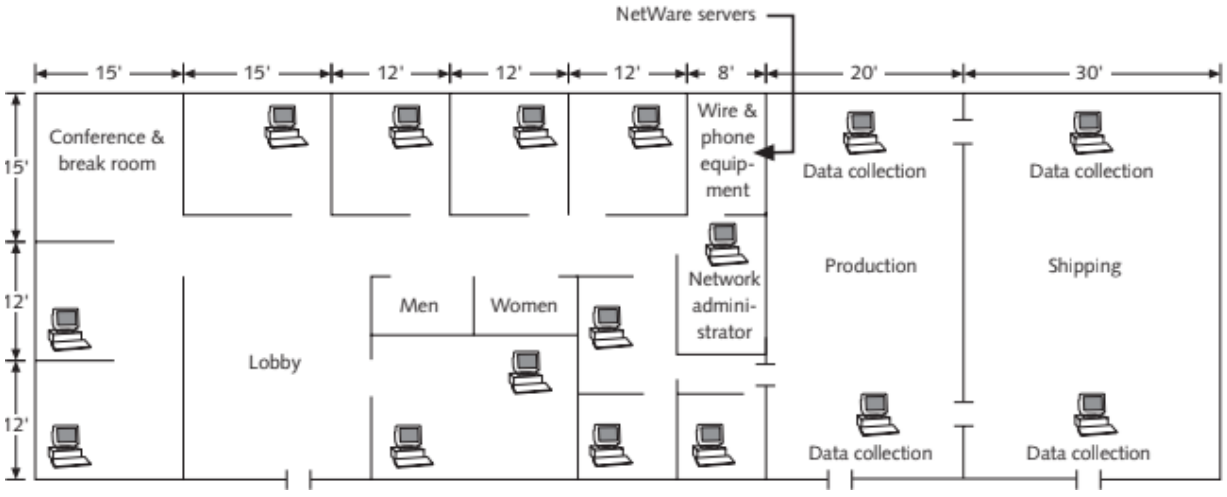

Fig 1.1: A Sample Floor Plan

Black Box Penetration Testing:

In this Method attacker is has no knowledge about the target as it exactly simulates an actual cyber attack where an actual black hat hacker attacks. This testing takes time as the attacker has no knowledge about the system so he gathers them. This method is used to find existing vulnerabilities in the system and used to simulate how far a hacker can go into the system without any information about the system.

Grey Box Penetration Testing:

In this method, the attacker is provided with a bit more information about the target like network configurations, subnets, or a specific IP to test. Attacker has a basic idea of how the machine is to which he/she is going to perform an attack, they may also be provided with low-level login credentials or access to the system which helps them in having a clear approach, This saves time of Reconnaissance the target.

Phases of Penetration Testing:

Penetration testing consists of 5 phases. They are:

- Reconnaissance
- Scanning
- Vulnerability Assessment
- Exploitation
- Reporting

Fig 1.2: Phases of Penetration Testing

1. Reconnaissance (Information Gathering):

In this phase, the tester gathers as much information about the target system as they can, including information about the network topology, operating systems and applications, user accounts,

and other relevant information. The goal is to gather as much data as possible so that the tester can plan an effective attack strategy.

Reconnaissance can be categorized as

- active reconnaissance
- passive reconnaissance

depending on what methods are used to gather information.

Active reconnaissance	Passive reconnaissance
Gathers information by directly interacting with the target system.	Gathers information from resources that are already publicly available.

2. Scanning:

The tester uses various tools to identify open ports and check network traffic on the target system. Because open ports are potential entry points for attackers, penetration testers need to identify as many open ports as possible for the next penetration testing phase.

3. Vulnerability Assessment:

The tester uses all the data gathered in the reconnaissance and scanning phases to identify potential vulnerabilities and determine whether they can be exploited. Much like scanning, vulnerability assessment is a useful tool on its own but is more powerful when combined with the other penetration testing phases.

4. Exploitation:

In this penetration testing phase, the penetration tester attempts to access the target system and exploit the identified vulnerabilities, typically by using a tool like Metasploit to simulate real-world attacks. This is perhaps the most delicate penetration testing phase because accessing the target system requires bypassing security restrictions.

5. Reporting:

Once the exploitation phase is complete, the tester prepares a report documenting the penetration test's findings. The report generated in this final penetration testing phase can be used to fix any vulnerabilities found in the system and improve the organization's security posture.

The report serves as a roadmap to guide the organization towards a more secure organization infrastructure.

Types of the Penetration test :

1. **Social Engineering Penetration test:-** This test can also be considered as a part of the Network Penetration Test. In this case, an organization might ask the penetration tester to attack its users.

This is the moment where the penetration tester eligible to use the speared phishing attack and more to trick the user to do unthinkable.

2. **Physical penetration test:-** In this case, the penetration tester will be asked to check the physical security controls of the building like locks and RFID mechanisms.
3. **Network penetration test:-** in this case, the penetration tester will have to test the network environment for potential security vulnerabilities and threats.
4. **Web Application penetration test:-** This test is nowadays considered to be common as application hosts data's which can be considered as critical as it can be. The data can be like the username, passwords, or more.
5. **Mobile Application penetration test:-** This test is done because every organization nowadays used Android or IoS mobile-based applications. So the goal is to make their mobile applications are secured and to make it reliable for the customer to provide personal information when they are using any applications.

Advantages of the Penetration test:

- The penetration test can be done to find the vulnerability which may serve as a weakness for the system.
- It is also done to identify the risks from the vulnerabilities.
- It can help determine the impact of an attack and the likelihood of it happening.
- It can help assess the effectiveness of security controls.
- It can help prioritize remediation efforts.
- It can provide assurance that the system is secure.
- It can be used to test the security of any system, no matter how large or small.
- It can be used to find vulnerabilities in systems that have not yet been exploited.
- It can be used to assess the effectiveness of security controls in place.
- It can be used to educate employees about security risks.

Disadvantages of the Penetration test:

- The penetration test which is not done properly can expose data that might be sensitive and more.
- The penetration tester has to be trusted, otherwise, the security measures taken can backfire.
- It is difficult to find a qualified penetration tester.
- Penetration testing is expensive.
- It can be disruptive to business operations.
- It may not identify all security vulnerabilities.
- It may give false positives (incorrectly identifying a vulnerability).

- It may give false negatives (failing to identify a vulnerability).
- It may require specialized skills and knowledge.
- The results may be difficult to interpret.
- After the penetration test is completed, the system is vulnerable to attack.

Penetration Testing Tools:

1. **Nmap:** It is a network exploration tool and security scanner. It can be used to identify hosts and services on a network, as well as security issues.
2. **Nessus:** It is a vulnerability scanner. It can be used to find vulnerabilities in systems and applications.
3. **Wireshark:** It is a packet analyzer. It can be used to capture and analyze network traffic.
4. **Burp Suite:** It is a web application security testing tool. It can be used to find security issues in web applications.

1.4 Laws of the Land

As a security tester, one must be aware of what they're allowed to do and what they should not or cannot do. For example, some security testers know how to pick a deadbolt lock, so a locked door wouldn't deter them from getting physical access to a server. However, testers must be knowledgeable about the laws for possessing lock-picks before venturing out to a corporate site with tools in hand. In fact, laws vary from state to state and country to country. In some states, the mere possession of lock-picking tools constitutes a crime, whereas other states allow possession as long as a crime hasn't been committed. In one state, they might be charged with a misdemeanor for possessing these tools; in another state, they might be charged with a felony.

As with lock-picking tools, having some hacking tools on a computer might be illegal. One should contact local law enforcement agencies and ask about the laws for their state or country before installing hacking tools on your computer.

Laws are written to protect society. Laws for having hacking tools that allow one to view a company's network infrastructure aren't as clearly defined as laws for possession of lock-picking tools because laws haven't been able to keep up with the speed of technological advances. In some states, running a program that gives an attacker an overview and a detailed description of a company's network infrastructure isn't seen as a threat. Some hackers use software to crack passwords of logon accounts. This act, performed by many security professionals when given permission to do so by a network's owner, is a federal offense when done without permission and can add substantial prison time to a hacker's sentence.

Table 1.1 An overview of recent hacking cases

State and Year	Description
California, 2008	Jon Paul Oson, a former IT network engineer and technical services manager for San Diego's Council of Community Health Clinics, was sentenced to 63 months in prison on federal hacking charges. He was convicted of intentionally damaging protected computers by disabling the backup database of patient information and deleting data and software on several servers.
California, 2009	Mario Azar, 28, an IT consultant for Pacific Energy Resources (PER), was indicted on federal charges of damaging the company's computer systems after it declined to offer him permanent employment. He was charged with unauthorized impairment of a protected computer, which carries a maximum penalty of 10 years in federal prison. Azar accessed PER computer systems illegally and caused thousands of dollars of damage to data.
Pennsylvania, 2009	University of Pennsylvania student Ryan Goldstein, 22, was sentenced to 3 months in prison and 5 years of probation for a hacking scheme that crashed an engineering school server. He helped a New Zealand hacker launch a 50,000 computer attack against online chat networks by using a botnet. With this attack, Goldstein was able to access the university's server illegally, which was used by more than 4000 students, faculty, and staff.

Table 1.2 Federal computer crime laws

Federal law	Description
The Computer Fraud and Abuse Act. Title 18, Crimes and Criminal Procedure. Part I: Crimes, Chapter 47, Fraud and False Statements, Sec. 1030: Fraud and related activity in connection with computers	This law makes it a federal crime to access classified information or financial information without authorization.
Electronic Communication Privacy Act. Title 18, Crimes and Criminal Procedure. Part I: Crimes, Chapter 119, Wire and Electronic Communications Interception and Interception of Oral Communications, Sec. 2510:	These laws make it illegal to intercept any communication, regardless of how it was transmitted.

Definitions and Sec. 2511: Interception and disclosure of wire, oral, or electronic communications prohibited	
Homeland Security Act of 2002, H.R. 5710, Sec. 225: Cyber Security Enhancement Act of 2002	This amendment to the Homeland Security Act of 2002 specifies sentencing guidelines for certain types of computer crimes.
The Computer Fraud and Abuse Act. Title 18, Crimes and Criminal Procedure, Sec. 1029: Fraud and related activity in connection with access devices	This law makes it a federal offense to manufacture, program, use, or possess any device or software that can be used for unauthorized use of telecommunications services.

As a security tester, you must be careful that your actions don't prevent the client's employees from doing their jobs. If you run a program that uses network resources to the extent that a user is denied access to them, you have violated federal law. For example, denial-of-service (DoS) attacks, should not be initiated on your client's networks.

Skills of a Security tester:

- **Knowledge of network and computer technology** - As a security tester, one must have a good understanding of networking concepts. They should spend time learning and reviewing TCP/IP and routing concepts and be able to read network diagrams. Being a security tester is impossible without a high level of expertise in this area. They should also have a good understanding of computer technologies and OSs.
- **Ability to communicate with management and IT personnel** - Security testers need to be good listeners and must be able to communicate verbally and in writing with members of management and IT personnel. Explaining the findings to CEOs might be difficult, especially if they don't have a technical background. Their reports should be clear and succinct and offer constructive feedback and recommendations.
- **An understanding of the laws that apply to their location** - As a security tester, one must be aware of what they can and can't do legally. Gathering this information can be difficult when working with global companies, as laws can vary widely in other countries.

- **Ability to apply the necessary tools to perform their tasks** - Security testers must have a good understanding of tools for conducting security tests. More important, they must be able to think outside the box by discovering, creating, or modifying tools when current tools don't meet their needs.

1.5 Overview of TCP/IP

For computers to communicate with one another over the Internet or across an office, they must speak the same language. This language is referred to as a protocol, and the most widely used is Transmission Control Protocol/Internet Protocol (TCP/IP). No matter what medium connects workstations on a network—copper wires, fibre-optic cables, or a wireless setup — the same protocol must be running on all computers if communication is going to function correctly.

TCP/IP Model:

The TCP/IP model refers to the Transmission Control Protocol/Internet Protocol Model. This model is a part of the network domain designed specifically for overseeing efficient and error-free transmission of data.

TCP/IP Features:

- Open protocol standards, freely available and developed independently from any specific computer hardware or operating system. Because it is so widely supported, TCP/IP is ideal for uniting different hardware and software components, even if you don't communicate over the Internet.
- Independence from specific physical network hardware. This allows TCP/IP to integrate many different kinds of networks. TCP/IP can be run over an Ethernet, a DSL connection, a dial-up line, an optical network, and virtually any other kind of physical transmission medium.
- A common addressing scheme that allows any TCP/IP device to uniquely address any other device in the entire network, even if the network is as large as the worldwide Internet.
- Standardized high-level protocols for consistent, widely available user services.

Layers of the TCP/IP Model:

The TCP/IP model is divided into four different layers:

- Application layer
- Transport layer
- Internet layer
- Network Access layer

Each layer performs a specific task on the data that is being transmitted over the network channel, and data moves from one layer to another in a preset pattern as mentioned below:

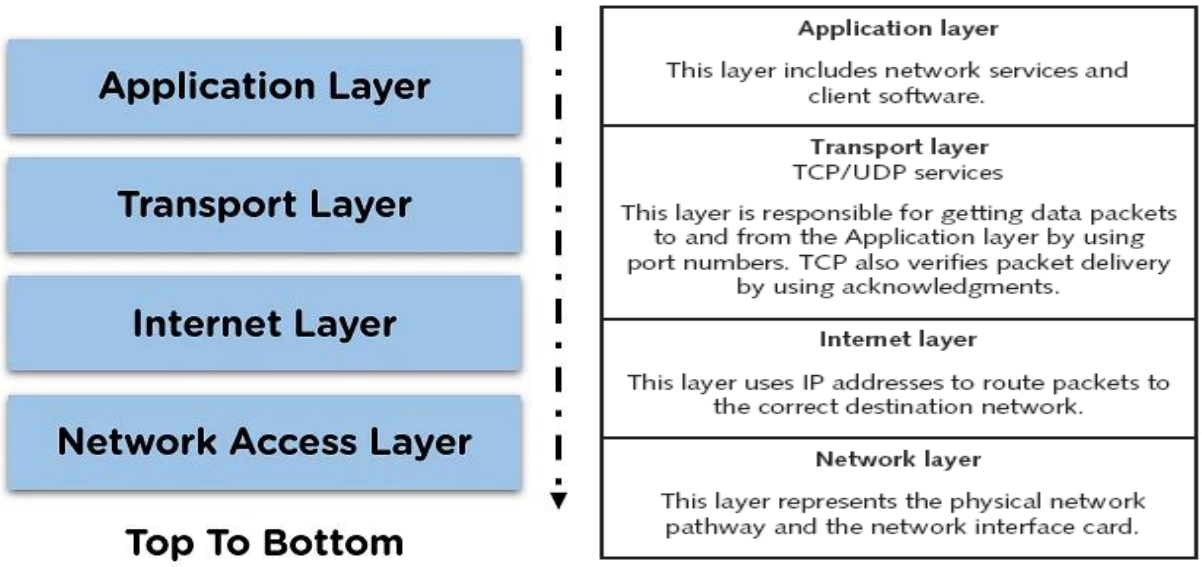

Fig 1.3: TCP / IP Layers

The above model represents the flow of data when it is being transmitted from the sender side. In the case of data being received, the layers of the model work in reverse order.

Functions of TCP/IP Layers:

The TCP/IP model is a four-layer model that divides network communications into four distinct categories or layers. The model is often referred to as the TCP/IP stack. The four important layers are the application layer, the transport layer, the network layer, and the link layer.

- **The Application Layer:** The application layer is closest to the end user. And this is the layer that users interact with directly, including protocols such as HTTP, FTP, and SSH. This layer is responsible for providing applications with access to the network.
- **The Transport Layer:** The transport layer ensures that data is delivered reliably and efficiently from one point to another. This layer handles data transmission between hosts, including protocols like TCP and UDP.
- **The Internet Layer:** The network layer is responsible for routing data through the web. This layer delivers data packets from one host to another, including the IP protocol.
- **The Link Layer:** The link layer provides reliable data links between the two nodes — for example, protocols like ethernet and Wi-Fi.

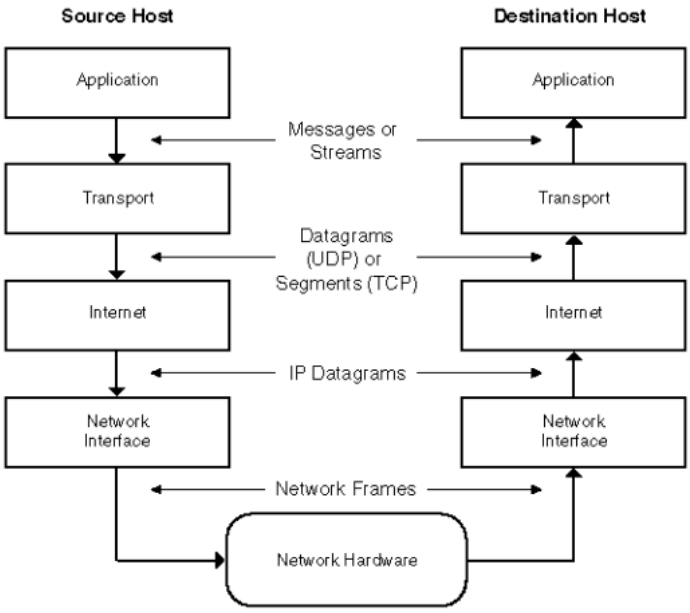

Fig 1.4: TCP / IP Model

Application Layer

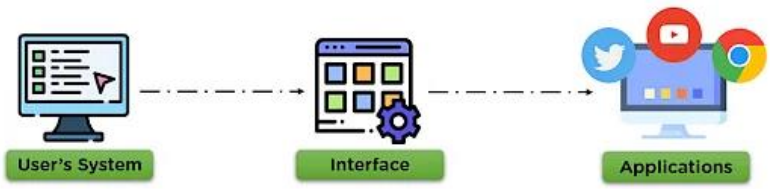

Fig 1.5: Application Layer

This is the topmost layer which indicates the applications and programs that utilize the TCP/IP model for communicating with the user through applications and various tasks performed by the layer, including data representation for the applications executed by the user and forwards it to the transport layer.

The application layer maintains a smooth connection between the application and user for data exchange and offers various features as remote handling of the system, e-mail services, etc.

Some of the protocols used in this layer are:

- **HTTP:** Hypertext transfer protocol is used for accessing the information available on the internet.
- **SMTP:** Simple mail transfer protocol, for transmitting e-mail messages across the internet.
- **FTP:** This is the standard protocol that allows different OSs to transfer files over the network channel.

- **Simple Network Management Protocol (SNMP):** Primarily used to monitor devices on a network, such as monitoring a router's state remotely.
- **Secure Shell (SSH)** - Enables a remote user to log on to a server securely and issue commands interactively.
- **Internet Relay Chat (IRC)** - Enables multiple users to communicate over the Internet in discussion forums.
- Telnet - Enables users to log on to a server remotely and issue commands interactively.

The functions of the application layer are −

- It facilitates the user to use the services of the network.
- It is used to develop network-based applications.
- It provides user services like user login, naming network devices, formatting messages, and e-mails, transfer of files etc.
- It is also concerned with error handling and recovery of the message as a whole.

Transport Layer

Fig 1.6: Transport Layer

This layer is responsible for establishing the connection between the sender and the receiver device and also performs the task of dividing the data from the application layer into packets, which are then used to create sequences.

It also performs the task of maintaining the data, i.e., to be transmitted without error, and controls the data flow rate over the communication channel for smooth transmission of data.

The protocols used in this layer are:

- **TCP:** Transmission Control Protocol is responsible for the proper transmission of segments over the communication channel. It also establishes a network connection between the source and destination system.

- **UDP:** User Datagram Protocol is responsible for identifying errors, and other tasks during the transmission of information. UDP maintains various fields for data transmission such as:
  - **Source Port Address:** This port is responsible for designing the application that makes up the message to be transmitted.
  - **Destination Port Address:** This port receives the message sent from the sender side.
  - **Total Length:** The total number of bytes of the user datagram.
  - **Checksum:** Used for error detection of the message at the destination side.

Internet Layer

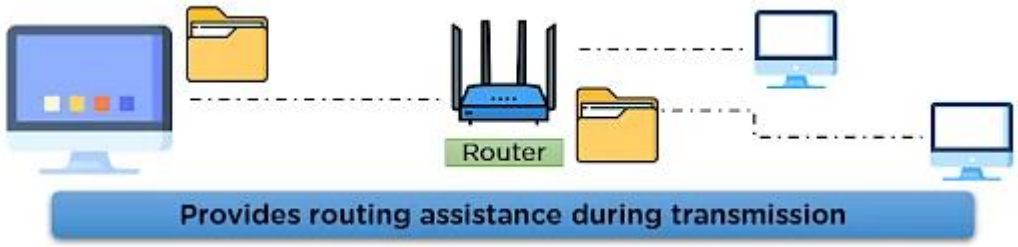

Fig 1.7: Internet Layer

The Internet layer performs the task of controlling the transmission of the data over the network modes and enacts protocols related to the various steps related to the transmission of data over the channel, which is in the form of packets sent by the previous layer.

This layer performs many important functions in the TCP/IP model, some of which are:

1. It is responsible for specifying the path that the data packets will use for transmission.
2. This layer is responsible for providing IP addresses to the system for the identification matters over the network channel.

Some of the protocols applied in this layer are:

- **IP**: This protocol assigns your device with a unique address; the IP address is also responsible for routing the data over the communication channel.
- **ARP:** This protocol refers to the Address Resolution Protocol that is responsible for finding the physical address using the IP address.

Network Access Layer

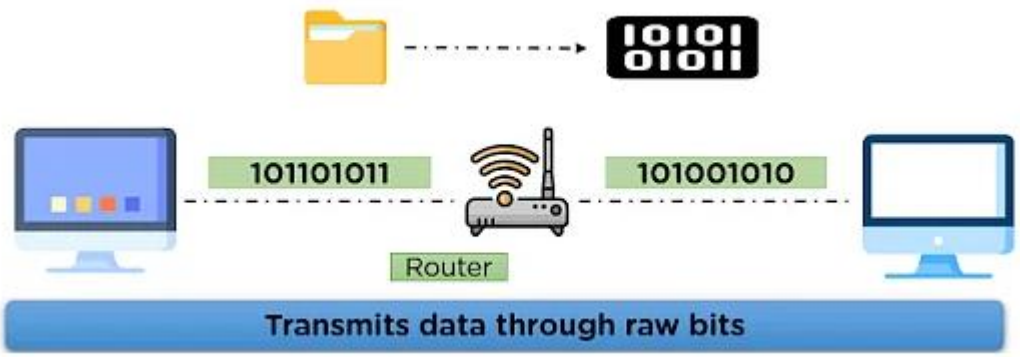

Fig 1.8: Network Layer

This layer is the combination of data-link and physical layer, where it is responsible for maintaining the task of sending and receiving data in raw bits, i.e., in binary format over the physical communication modes in the network channel.

- It uses the physical address of the system for mapping the path of transmission over the network channel.

Advantages of TCP/IP:

- **Scalability:** The TCP/IP model is highly scalable and can accommodate small and large networks.
- **Reliability:** The model is robust and reliable, making it suitable for mission-critical applications.
- **Flexibility:** It is very flexible, allowing for interoperability between different types of networks.
- **Security:** The various protocols in the model provide robust security measures.
- **Cost-effectiveness:** TCP/IP is relatively inexpensive to implement and maintain.

Disadvantages of TCP/IP:

- **Complexity:** The model is quite complex and requires a certain degree of expertise to configure and maintain.
- **Vulnerability:** Because of its complexity, it is vulnerable to attack.
- **Performance:** Performance can be degraded due to network congestion and latency.

Uses of TCP/IP:

Here are some of the most valuable uses of TCP/IP models:

- **World Wide Web:** TCP/IP transfers data between web browsers and servers.
- **Email:** Applications such as Outlook, Thunderbird, and Gmail use TCP/IP protocols to send and receive emails.
- **File Transfer:** FTP, SFTP, and other file transfer services rely on TCP/IP to move files from one computer to another.

- **Networking:** TCP/IP links computers together in a network.
- **Virtual Private Networks:** VPNs use TCP/IP to encrypt data before it travels across a public or private network.
- **Internet of Things:** Many smart home devices use TCP/IP to communicate and transfer data.
- **Voice Over Internet Protocol:** VOIP services such as Skype and Google Voice use TCP/IP to transmit calls over the internet.

1.6 IP Addressing

An IP address is an address having information about how to reach a specific host, especially outside the LAN (Local Area Network). An IP address is a 32-bit unique address having an address space of 2^{32}.Generally, there are two notations in which the IP address is written, dotted decimal notation and hexadecimal notation.

i. Dotted Decimal Notation:

A dotted decimal notation should have the following:

1. The value of any segment (byte) is between 0 and 255 (both included).
2. No zeroes are preceding the value in any segment (054 is wrong, 54 is correct).

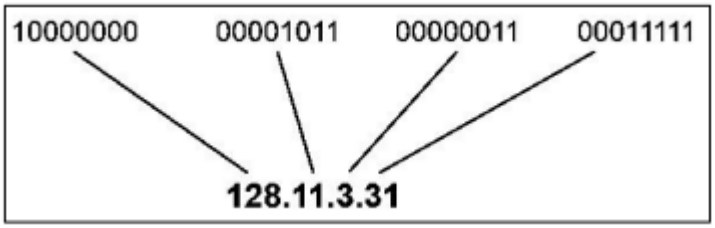

Fig 1.9: Dotted decimal notation

ii. Hexadecimal Notation:

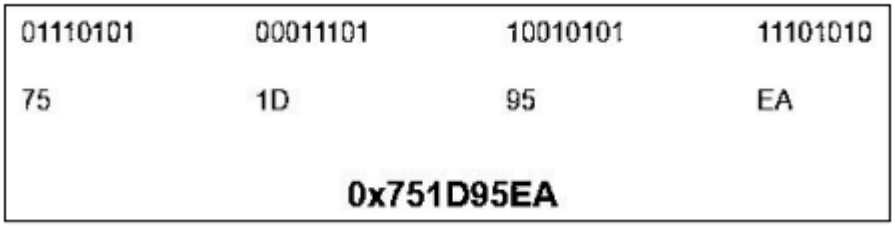

Fig 1.10: Hexadecimal notation

(i) Classful addressing:

The 32 - bit IP address is divided into five sub-classes. These are:

- Class A
- Class B
- Class C
- Class D
- Class E

Each of these classes has a valid range of IP addresses. **Classes D and E** are reserved for **multicast and experimental purposes** respectively. The order of bits in the first octet determines the classes of the IP address. The IPv4 address is divided into two parts:

- Network ID
- Host ID

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each network administrator assigns an IP address to each device that is connected to its network.

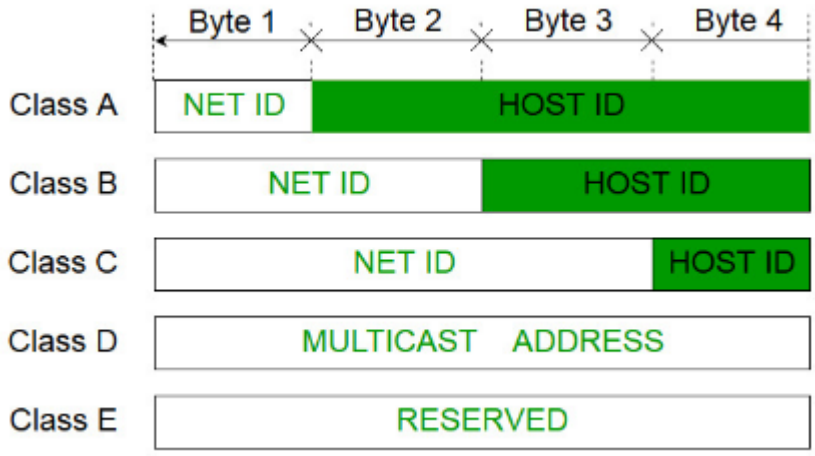

Fig 1.11: Classful addressing

Class A:

IP addresses belonging to class A are assigned to the networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

The higher-order bit of the first octet in class A is always set to **0**. The remaining 7 bits in the first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for Class A is 255.x.x.x. Therefore, class A has a total of:

- 2 ^ 7 - 2 = 126 network ID (Here 2 address is subtracted because 0.0.0.0 and 127.x.y.z are special address.)

- 2 ^ 24 - 2 = 16,777,214 host ID

IP addresses belonging to class A ranges from 1.x.x.x - 126.x.x.x

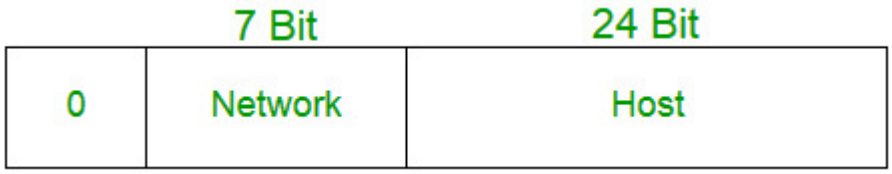

Fig 1.12: Class A

Class B:

IP address belonging to class B is assigned to networks that range from medium-sized to large-sized networks.

- The network ID is 16 bits long.
- The host ID is 16 bits long.

The higher-order bits of the first octet of IP addresses of class B are always set to **10**. The remaining 14 bits are used to determine the network ID. The 16 bits of host ID are used to determine the host in any network. The default subnet mask for class B is 255.255.x.x. Class B has a total of:

- 2^14 = 16384 network address
- 2^16 – 2 = 65534 host address

IP addresses belonging to class B ranges from 128.0.x.x - 191.255.x.x.

Fig 1.13: Class B

Class C:

IP addresses belonging to class C are assigned to small-sized networks.

- The network ID is 24 bits long.
- The host ID is 8 bits long.

The higher-order bits of the first octet of IP addresses of class C is always set to **110**. The remaining 21 bits are used to determine the network ID. The 8 bits of host ID are used to determine the host in any network. The default subnet mask for class C is 255.255.255.x. Class C has a total of:

- 2^21 = 2097152 network address

- 2^8 – 2 = 254 host address

IP addresses belonging to class C range from 192.0.0.x - 223.255.255.x.

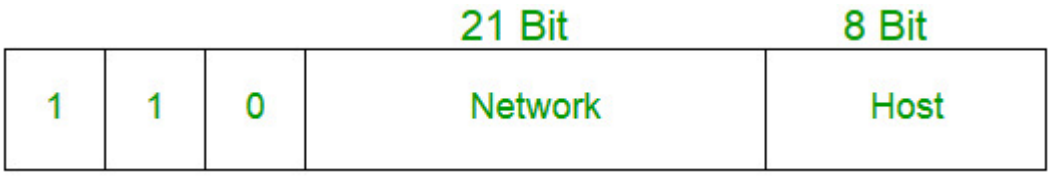

Fig 1.14: Class C

Class D:

IP address belonging to class D is reserved for **multi-casting**. The higher-order bits of the first octet of IP addresses belonging to class D is always set to **1110**. The remaining bits are for the address that interested hosts recognize.

Class D does not possess any subnet mask. IP addresses belonging to class D range from 224.0.0.0 - 239.255.255.255.

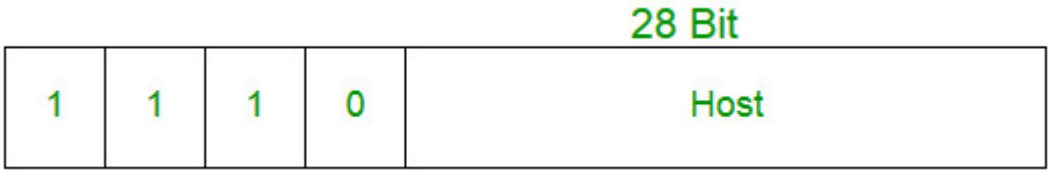

Fig 1.15: Class D

Class E:

IP addresses belonging to class E are reserved for **experimental and research purposes**. IP addresses of class E range from 240.0.0.0 - 255.255.255.254. This class doesn't have any subnet mask. The higher-order bits of the first octet of class E are always set to **1111**.

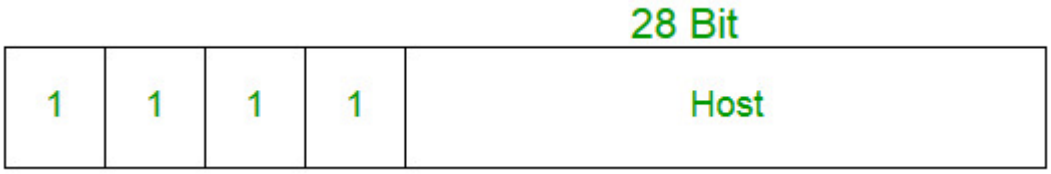

Fig 1.16: Class E

(ii) Classless addressing:

The problem with the classful addressing method is that millions of class A addresses are wasted, many of the class B addresses are wasted, whereas, the number of addresses available in class C is so small that it cannot cater to the needs of organizations. Class D addresses are used for

multicast routing and are therefore available as a single block only. Class E addresses are reserved. Since there are these problems, Classful networking was replaced by **Classless Inter-Domain Routing (CIDR)**.

To reduce the wastage of IP addresses in a block, **sub-netting**is used. The IP address will be given and the number of bits for mask are defined along with it, like, 192.168.1.1/28. Here, **subnet mask** is found by putting the given **number of bitsout of 32 as 1**, like, in the given address, **28 out of 32 bits**need to be set as 1 and the rest as 0, and so, the **subnet mask** would be **255.255.255.240**.

Network address:

It identifies a network on internet. Using this, the range of addresses in the network and totalpossible number of hosts in the network can be found.

Mask:

It is a 32-bit binary number that gives the network address in the address block when AND operation is bitwise applied on the mask and any IP address of the block.

The default mask in different classes are :

Class A	Class B	Class C
255.0.0.0	255.255.0.0	255.255.255.0

Problem: If the IP address is 132.6.17.85, then find the network address.

Solution: The default mask is 255.255.0.0, which means that only the first 2 bytes are preserved and the other 2 bytes are set to 0. Therefore, the network address is **132.6.0.0**.

Subnetting:

Dividing a large block of addresses into several contiguous sub-blocks and assigning these sub-blocks to different smaller networks is called subnetting. It is a practice that is widely used when classless addressing is done.

Some values calculated in subnetting:

1. Number of subnets : $2^{(\text{Given bits for mask - No. of bits in default mask})}$

2. Subnet address : AND result of subnet mask and the given IP address

3. Broadcast address : By putting the host bits as 1 and retaining the network bits as in the IP address

4. Number of hosts per subnet : $2^{(32 - \text{Given bits for mask})} - 2$

5. First Host ID : Subnet address + 1 (adding one to the binary representation of the subnet address)

6. Last Host ID : Subnet address + Number of Hosts

Problem: If the IP Address is 172.16.0.0/25, then find the number of subnets and the number of hosts per subnet. Also, for the first subnet block, find the subnet address, first host ID, last host ID, and broadcast address.

Solution: This is a class B address. So, no. of subnets = $2^{(25-16)} = 2^9 = 512$.

No. of hosts per subnet = $2^{(32-25)} - 2 = 2^7 - 2 = 128 - 2 = 126$.

For the first subnet block, we have subnet address = 172.16.0.0.

First host id = 172.16.0.1.

Last host id = 172.16.0.126.

and Broadcast address = 172.16.0.127.

1.7 Network and Computer Attacks

Network Attack:

A network attack include

- unauthorized attempts to access network resources or systems,
- attempts to destroy or corrupt information, and
- attempts to prevent authorized users from accessing resources.

Network attacks can be classified into several categories,

- depending on the method used
- the target
- the intent of the attacker.

One way to **classify network attacks is by their intent**. Some attacks are designed to disrupt the normal operation of a network or its resources, while others are designed to steal sensitive information or take control of network resources.

Another way to **classify network attacks is by the method used**. Some attacks involve exploiting known vulnerabilities in network software or hardware, while others use social engineering techniques to trick users into revealing sensitive information.

There are **two main types of network attacks**:

- **Passive:** Attackers gain access to a network and can monitor or steal sensitive information, but without making any change to the data, leaving it intact.
- **Active:** Attackers not only gain unauthorized access but also modify data, either deleting, encrypting or otherwise harming it.

Computer Attack:

A cyber attack or computer attack is any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage. Cyber attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems.

Network security:

Network Security protects data and systems from unauthorized access, unwanted modification, intrusions, and other threats because unauthorized persons or attackers can penetrate the data, expose personal information, or steal money. It defends network traffic and protects the infrastructure from numerous threats, including trojan horses, malware, etc

MALWARE – short for malicious software which is specifically designed to disrupt, damage, or gain authorized access to a computer system. Much of the malware out there today is self-replicating: once it infects one host, from that host it seeks entry into other hosts over the Internet, and from the newly infected hosts, it seeks entry into yet more hosts. In this manner, self-replicating malware can spread exponentially fast.

Malware is software that infects computer systems to damage, disable or exploit the computer or network to:

- Steal, encrypt or delete sensitive information
- Hijack or alter core system functions
- Monitor user activity without permission
- Extort money
- Introduce spam or forced advertising

There are several major types of malware to keep an eye out for:

- **Adware** — Adware is a type of malicious software that secretly installs itself on your device and automatically delivers unwanted advertisements to generate revenue for its creator or a third party. It is often used in conjunction with spyware.
- **Backdoor (trapdoor)** — A backdoor allows cybercriminals to access a computer without the user's knowledge. Backdoors are meant for future use and can remain in a system for years without being noticed.
- **Rogueware** — Rogueware misleads users into believing their device is infected so they will click on a fake warning, which promptly installs malware.
- **Ransomware** — Ransomware restricts users from accessing a system or its data, and often threatens to publish or delete data, until ransom is paid. Locker ransomware restricts access to the infected device, while crypto ransomware restricts access to stored data and files.
- **Spyware** — Spyware is malicious software that enters a user's computer, designed to gather information from the device and user. Once installed, it can log keystrokes and extract sensitive information. Spyware can also enable hackers to watch and listen through cameras and microphones.
- **Trojan horse** — it is a type of malware that typically gets hidden as an attachment in an email or a free-to-download file, then transfers onto the user's device. Once downloaded, the malicious code will execute the task the attacker designed it for, such as gain backdoor access to corporate systems, spy on users' online activity, or steal sensitive data.
- **Virus** — The oldest type of malware, viruses alters the way a computer operates. A virus can replicate itself and spread to other devices, but it must be attached to another program or executed by a user action.
- **Worm** — Worms are the most common type of malware and one of the most dangerous, because they can replicate themselves without being attached to a program or run by a user.
- **Man-in-the-middle** - A Man-in-the-middle (MITM) attack occurs when an attacker stands between two devices or between a client and a server, intercepts, monitors, and steals confidential data, or modifies it and sends it back to the original receiver.
- **Phishing** - A phishing attack is a social engineering attack. An attacker manipulates the victim's thoughts to get personal information like credit and debit cards, online banking details, username and password, social networking information, and other digital account information. Phishing is the term used nowadays when a hacker or attacker tries to deceive individuals by threatening, frightening, or seducing them. Attackers send malicious attachments and links to users via email, posing as trusted sources such as company owners, managers, or bankers. When users open the email with interest, they allow access to the attackers.

- **IP Spoofing -** IP (Internet Protocol) Spoofing is a form of malicious attack. Spoofing is a DDoS and Man-in-the-Middle attack technique used by attackers on target devices. The attacker keeps track of the system's packet header information, such as IP address and Mac address, and then replaces the source IP address with a spoofed IP address to impersonate the sender's true identity. The receiver will believe it interacts with a trusted source and provides access to the attacker. Hackers take advantage of spoofed IP packets because they know these are the primary way of transmitting data between sender and recipient.
- **Packet Sniffer -** Packet sniffers capture or save copies of each transmission packet when packets flow over a network in a wireless transmission zone. A sniffer is a tool attackers use to gather sensitive information such as social information, financial data, trade secrets, user IDs, passwords, etc. Sniffing is a data theft technique that involves capturing, decoding, inspecting, and interpreting the information contained within a network packet on a TCP/IP connection using a packet sniffer

Common computer viruses

Virus	Description
Gumblar	First detected in March 2009, it spread by mass hacking of hundreds of thousands of Web sites, which then exploited visiting browsers via Adobe PDF and Flash vulnerabilities. The malware steals FTP credentials that are used to further compromise Web sites the victim maintains. It also hijacks Google searches and blocks access to antivirus update sites to prevent removal. Recent variations install a backdoor that attempts to connect to a botnet.
Luckysploit	It's actually the attack side of a sophisticated cybercrime toolkit that spreads when Web surfers visit a hacked Web site hosting the malware. It uses obfuscated JavaScript code and asymmetric key encryption to prevent detection. The JavaScript code also targets victims based on recent vulnerabilities in OSs, applications, browser plug-ins, and so on.
Zlob	Purported to be the work of the Russian Business Network, Zlob has dozens of variants, some of which spread by masquerading as a codec needed to view an enticing video. Several variants are associated with "scareware," fake antivirus downloads that change home router settings to redirect victims to more malicious sites.
Gpcode	This "ransomware" virus detected in 2008 isn't widespread but is unique because it uses practically unbreakable 1024-bit asymmetric key encryption to hide a user's documents on the computer and hold them for ransom until the victim pays to get the encryption key.

Common computer worms

Worm	Description
Storm	Detected in January 2007, it's spread by automatically generated e-mail messages. It's estimated that this botnet Trojan program and its variants infected millions of systems.
Mytob	Detected in 2005, it's a hybrid worm with backdoor capabilities spread by mass e-mailing and exploiting Windows vulnerabilities.
Waledac	This e-mail worm harvests and forwards passwords and spreads itself in an e-mail with an attachment called eCard.exe. It has many variants that can be controlled remotely. A recent variant uses a geographic IP address lookup to customize the e-mail message so that it looks like a Reuters news story about a dirty bomb that exploded in a city near the victim.
Conficker	Detected in late 2008, this botnet worm and its variants propagated through the Internet by using a Microsoft network service vulnerability. It updates itself dynamically but can be detected remotely with a standard port scanner, such as Nmap, and a special Conficker signature plug-in.
Mod_ssl	Detected in 2002, this worm affects Linux systems running Apache OpenSSL. It scans for vulnerable systems on TCP port 80 and attempts to deliver the exploit code through TCP port 443. A system infected with this worm begins spreading it to other systems on a network. See VU#102795 and CA-2002-23 at *www.kb.cert.org/vuls* for more information; this site cross-references vulnerabilities listed at *www.cve.mitre.org*.
Slammer	Detected in 2003, this worm was purported to have shut down more than 13,000 ATMs of one of the largest banks in America by infecting database servers located on the same network.

1.8 Protecting Against Malware Attacks

There are no ways to prevent malware attacks but there are reliable ways to detect and block attacks, thus protecting your systems from being infected by malicious software.

1. Install anti-virus and anti-spyware software.

Anti-virus and anti-spyware programs scan computer files to identify and remove malware. Be sure to:

- Keep your security tools updated.
- Immediately remove detected malware.
- Audit your files for missing data, errors, and unauthorized additions.

2. Use secure authentication methods.

The following best practices help keep accounts safe:

- Require strong passwords with at least eight characters, including an uppercase letter, a lowercase letter, a number and a symbol in each password.
- Enable multi-factor authentication, such as a PIN or security questions in addition to a password.
- Use biometric tools like fingerprints, voiceprints, facial recognition and iris scans.
- Never save passwords on a computer or network. Use a secure password manager if needed.

3. Use administrator accounts only when absolutely necessary.

Malware often has the same privileges as the active user. Non-administrator accounts are usually blocked from accessing the most sensitive parts of a computer or network system. Therefore:

- Avoid using administrative privileges to browse the web or check email.
- Log in as an administrator only to perform administrative tasks, such as to make configuration changes.
- Install software using administrator credentials only after you have validated that the software is legitimate and secure.

4. Keep software updated.

No software package is completely safe against malware. However, software vendors regularly provide patches and updates to close whatever new vulnerabilities show up. As a best practice, validate and install all new software patches:

- Regularly update your operating systems, software tools, browsers and plug-ins.
- Implement routine maintenance to ensure all software is current and check for signs of malware in log reports.

5. Control access to systems.

There are multiple ways to regulate your networks to protect against data breaches:

- Install or implement a firewall, intrusion detection system (IDS) and intrusion prevention system (IPS).
- Never use unfamiliar remote drives or media that was used on a publicly accessible device.
- Close unused ports and disable unused protocols.
- Remove inactive user accounts.
- Carefully read all licensing agreements before installing software.

6. Adhere to the least-privilege model.

Adopt and enforce the principle of least-privilege: Grant users in your organization the minimum access to system capabilities, services and data they need to complete their work.

7. Limit application privileges.

A hacker only needs an open door to infiltrate your business. Limit the number of possible entryways by restricting application privileges on your devices. Allow only the application features and functions that are absolutely necessary to get work done.

8. Implement email security and spam protection.

Email is an essential business communication tool, but it's also a common malware channel. To reduce the risk of infection:

- Scan all incoming email messages, including attachments, for malware.
- Set spam filters to reduce unwanted emails.
- Limit user access to only company-approved links, messages and email addresses.

9. Monitor for suspicious activity.

Monitor all user accounts for suspicious activity. This includes:

- Logging all incoming and outgoing traffic
- Baselining normal user activity and proactively looking for aberrations
- Investigating unusual actions promptly

10. Educate your users.

At the end of the day, people are the best line of defense. By continually educating users, you can help reduce the risk that they will be tricked by phishing or other tactics and accidentally introduce malware into your network. In particular:

- Build awareness of common malware attacks.
- Keep users up to date on basic cybersecurity trends and best practices.
- Teach users how to recognize credible sites and what to do if they stumble onto a suspicious one.
- Encourage users to report unusual system behavior.
- Advise users to only join secure networks and to use VPNs when working outside the office.

1.9 Intruder Attacks

The most common threat to security is the attack by the intruder. Intruders are often referred to as hackers and are the most harmful factors contributing to the vulnerability of security. They have immense knowledge and an in-depth understanding of technology and security. Intruders breach the privacy of users and aim at stealing the confidential information of the users. The stolen information is

then sold to third-party, which aim at misusing the information for their own personal or professional gains.

Categories of intruders:

(i) Masquerader:

The category of individuals that are not authorized to use the system but still exploit user's privacy and confidential information by possessing techniques that give them control over the system, such category of intruders is referred to as Masquerader. Masqueraders are outsiders and hence they don't have direct access to the system, their aim is to attack unethically to steal data/ information.

(ii) Misfeasor:

The category of individuals that are authorized to use the system, but misuse the granted access and privilege. These are individuals that take undue advantage of the permissions and access given to them, such category of intruders is referred to as Misfeasor. Misfeasors are insiders and they have direct access to the system, which they aim to attack unethically for stealing data/ information.

(iii) Clandestine User:

The category of individuals those have supervision/administrative control over the system and misuse the authoritative power given to them. The misconduct of power is often done by superlative authorities for financial gains, such a category of intruders is referred to as Clandestine User. A Clandestine User can be any of the two, insiders or outsiders, and accordingly, they can have direct/ indirect access to the system, which they aim to attack unethically by stealing data/ information.

Denial of Service (DoS) attacks

A Denial of Service (DoS) attack is an attempt to make a network resource or service unavailable to legitimate users by overwhelming it with traffic from multiple sources. The goal of a DoS attack is to disrupt the normal operation of a network or website, making it unavailable to legitimate users.

DoS attacks can be launched from a single machine or from a distributed network of compromised machines, known as a botnet. These attacks are relatively easy to launch and can cause significant disruption, even if the attack is not particularly sophisticated.

A DoS attack renders a network, host, or other pieces of infrastructure unusable by legitimate users. Most Internet DoS attacks fall into one of three categories :

- ***Vulnerability attack*:** This involves sending a few well-crafted messages to a vulnerable application or operating system running on a targeted host. If the right sequence of packets is

sent to a vulnerable application or operating system, the service can stop or, worse, the host can crash.

- ***Bandwidth flooding*:** The attacker sends a deluge of packets to the targeted host—so many packets that the target's access link becomes clogged, preventing legitimate packets from reaching the server.
- ***Connection flooding*:** The attacker establishes a large number of half-open or fully open TCP connections at the target host. The host can become so bogged down with these bogus connections that it stops accepting legitimate connections.

Distributed Denial of Service (DDoS) attacks

A Distributed Denial of Service (DDoS) attack is a type of attack that is similar to a Denial of Service (DoS) attack, but it uses a distributed network of compromised machines to generate traffic to overwhelm a target. This makes DDoS attacks much more difficult to defend against than traditional DoS attacks because the traffic is coming from multiple sources, making it difficult to distinguish legitimate traffic from attack traffic.

In a DDoS attack, an attacker infects a large number of computers with malware, creating a botnet, and then uses this botnet to generate a large amount of traffic directed at a target, such as a website or a network. The traffic can come in many forms, including HTTP requests, ICMP packets, and UDP traffic, among others. The goal is to saturate the network and resources of the target, making it unavailable to legitimate users.

Botnets:

Attackers build a network of hacked machine which are known as botnets, by spreading malicious piece of code through emails, websites and social media. Once these computers are infected, they can be controlled remotely without their owner's knowledge and used like an army to launch an attack against any target.

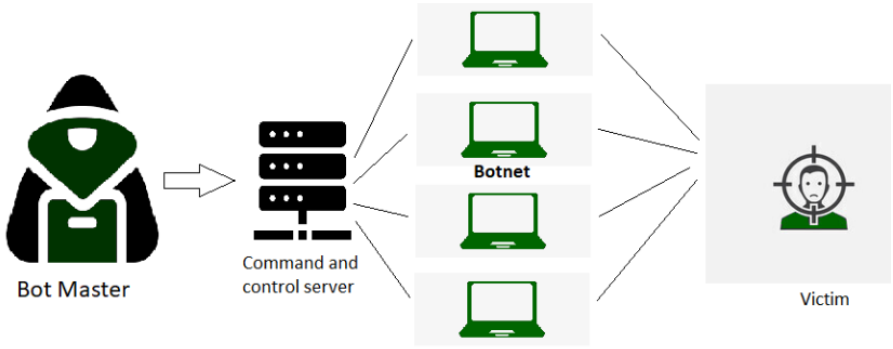

Fig.1.17: Botnet

Difference between DoS and DDoS:

DoS	DDoS
DoS Stands for Denial of service attack.	DDoS Stands for Distributed Denial of service attack.
In Dos attack single system targets the victim system.	In DDoS multiple systems attack the victim's system.
Victim's PC is loaded from the packet of data sent from a single location.	Victim PC is loaded from the packet of data sent from Multiple locations.
Dos attack is slower as compared to DDoS.	A DDoS attack is faster than Dos Attack.
Can be blocked easily as only one system is used.	It is difficult to block this attack as multiple devices are sending packets and attacking from multiple locations.
In DOS Attack only a single device is used with DOS Attack tools.	In a DDoS attack, The volumeBots are used to attack at the same time.
DOS Attacks are Easy to trace.	DDOS Attacks are Difficult to trace.
Types of DOS Attacks are: 1. Buffer overflow attacks 2. Ping of Death or ICMP flood 3. Teardrop Attack 4. Flooding Attack	Types of DDOS Attacks are: 1. Volumetric Attacks 2. Fragmentation Attacks 3. Application Layer Attacks 4. Protocol Attack.

Buffer Overflow Attack

A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

Attackers exploit buffer overflow issues by overwriting the memory of an application. This changes the execution path of the program, triggering a response that damages files or exposes private information. For example, an attacker may introduce extra code, sending new instructions to the application to gain access to IT systems.

Fig.1.18: Buffer Overflow Example

If attackers know the memory layout of a program, they can intentionally feed input that the buffer cannot store, and overwrite areas that hold executable code, replacing it with their own code. For example, an attacker can overwrite a pointer (an object that points to another area in memory) and point it to an exploit payload, to gain control over the program.

Types of Buffer Overflow Attacks

- **Stack-based buffer overflows** are more common, and leverage stack memory that only exists during the execution time of a function.
- **Heap-based attacks** are harder to carry out and involve flooding the memory space allocated for a program beyond memory used for current runtime operations.

Ping of Death (PoD) Attack

A Ping of death (PoD) attack is a denial-of-service (DoS) attack, in which the attacker aims to disrupt a targeted machine by sending a packet larger than the maximum allowable size, causing the target machine to freeze or crash.

The attacker simply creates an Internet Control Message Protocol (ICMP) packet that's larger than the maximum allowed 65,535 bytes. The large packet is fragmented into smaller packets and reassembled at its destination. The user's system at the destination point can't handle the reassembled oversized packet, thereby causing the system to crash or freeze.

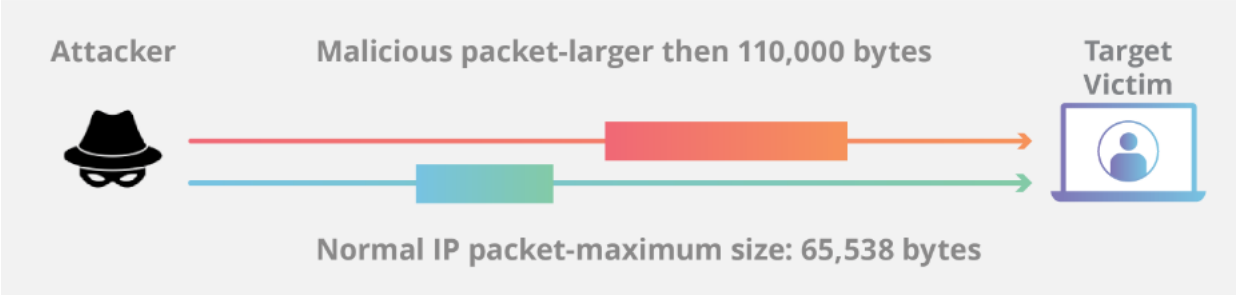

Fig.1.19: Ping of Death

Methods adopted by intruders for cracking passwords:

- Regressively try all short passwords that may open the system for them.

- Try unlocking the system with default passwords, which will open the system if the user has not made any change to the default password.
- Try unlocking the system by personal information of the user such as their name, family member names, address, phone number in different combinations.
- Making use of Trojan horse for getting access to the system of the user.
- Attacking the connection of the host and remote user and getting entry through their connection gateway.
- Trying all the applicable information, relevant to the user such as plate numbers, room numbers, locality info.

To prevent intruders from attacking the computer system, it is extremely important to be aware of the preventive measures which leads to strengthening of the security posture. Also, whenever there is potential detection of the system being attacked make sure to reach cyber security experts as soon as possible.

Burp Intruder:

Burp Intruder is a tool for automating customized attacks against web applications. It enables one to configure attacks that send the same HTTP request over and over again, inserting different payloads into predefined positions each time.

1.10 Addressing Physical Security

Protecting a network from attacks is not always a software issue. We should have some basic skills in protecting a network from physical attacks as well. No matter how effective the firewall is, we must secure servers and computers from an attack from within the organization. In fact, there's a higher chance that an attacker who breaks into the network is from inside the company rather than outside.

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism. While most of these are covered by insurance, physical security's prioritization of damage prevention avoids the time, money and resources lost because of these events. In terms of cybersecurity, the purpose of physical security is to minimize this risk to information systems and information. Systems and devices can provide threat actors with additional attack vectors to connect to networks, infect other devices, and exfiltrate data; therefore, access to systems, equipment, and respective operating environments should be limited to only authorized individuals. Multiple layers of physical security can be implemented to protect the most critical assets and services. There are four categories of **physical access security**

zones: public, reception, operations, and restricted access. Physical access controls can be implemented in accordance with these security zones, including barriers, security guards, security cameras, physical access devices, and identity and authorization controls. In addition, sensitive information, whether in paper or electronic form, must be protected from unauthorized access and disclosure.

Components of Physical security framework:

The success of an organization's physical security program can often be attributed to how well each of the below components is implemented, improved and maintained.

1. Access control

2. Surveillance

3. Testing

1. Access control:

The key to maximizing one's physical security measures is to limit and control what people have access to sites, facilities and materials. Access control encompasses the measures taken to limit exposure of certain assets to authorized personnel only. Examples of these corporate barriers often include ID badges, keypads and security guards. However, these obstacles can vary greatly in terms of method, approach and cost.

The building is often the first line of defense for most physical security systems. Items such as fences, gates, walls and doors all act as physical deterrents to criminal entry. Additional locks, barbed wire, visible security measures and signs all reduce the number of casual attempts carried out by cybercriminals. More sophisticated access controls involve a technology-supported approach. ID card scanners and near-field communication (NFC) ID cards are methods of physical authentication that security teams can use to verify the identities of individuals entering and exiting various facilities.

Using tactically placed obstacles, organizations can make it more difficult for attackers to access valuable assets and information. Similarly, these barriers increase the time it takes for threat actors to successfully carry out acts of thievery, vandalism or terrorism. The more obstacles that are in place, the more time organizations have to respond to physical security threats and contain them.

But criminals are not the only threat that access controls can minimize. Barriers such as walls and fences can also be used to harden buildings against environmental disasters, such as earthquakes, mud slides and floods. These risks are extremely location-dependent. Organizations that divert resources toward such hardening measures should balance the cost and benefit of their implementation prior to investment.

2. Surveillance:

This is one of the most important physical security components for both prevention and post-incident recovery. Surveillance refers to the technology, personnel and resources that organizations use to monitor the activity of different real-world locations and facilities. These examples can include **patrol guards, heat sensors and notification systems.**

The most common type of surveillance is **Closed Circuit Television (CCTV) cameras** that record the activity of a combination of areas. The benefit of these surveillance cameras is that they are as valuable in capturing criminal behavior as they are in preventing it. Threat actors who see a CCTV camera are less inclined to break in or vandalize a building out of fear of having their identity recorded. Similarly, if a particular asset or piece of equipment is stolen, surveillance can provide the visual evidence one needs to identify the culprit and their tactics.

3. Testing:

Physical security is a preventative measure and incident response tool. Disaster recovery(DR) plans ,for example, center on the quality of one's physical security protocols - how well a company identifies, responds to and contains a threat. The only way to ensure that such DR policies and procedures will be effective when the time comes is to implement active testing.

Testing is increasingly important, especially when it comes to the unity of an organization. Fire drills are a necessary activity for schools and buildings because they help to coordinate large groups, as well as their method of response. These policy tests should be conducted on a regular basis to practice role assignments and responsibilities and minimize the likelihood of mistakes

Keyloggers

Keyloggers are **hardware devices or software** that can be used to capture keystrokes on a computer.

Software keyloggers behave like Trojan programs and are loaded on a computer.

A hardware keylogger is a small device, often smaller than an inch long. It can usually be installed in less than 30 seconds. It's a simple matter of unplugging the keyboard, plugging the small device into the keyboard input jack, and then plugging the keylogger jack into the computer's keyboard port. After installing the hardware, most vendors require you to run a word processing program, such as WordPad, and then enter the vendor-supplied password in a blank document. After entering the password, a menu is displayed. Some common hardware keyloggers are **KeyKatcher and KeyGhost**.

KeyKatcher and KeyGhost can be quite useful when conducting a security test or penetration test for a company and can be installed and configured in a few minutes. KeyKatcher and KeyGhost were created for companies or even parents who want to monitor computers.

Unfortunately, attackers can also use keylogger devices. An unscrupulous employee can connect a keylogger to a manager's computer and retrieve confidential information later. Installing this device does require access to the computer, which might pose a problem if the manager's office is locked. However, as mentioned, keyloggers are also available as software (spyware) that's loaded on a computer, and retrieved information can be e-mailed or transferred to a remote location.

Beyond Locked Doors

The security professional should be aware of the types of locks used to secure a company's assets. If intruders can sit in front of your server, they can hack it. Simply put, **lock up your server**.

Attackers can find countless articles about lock picking. One paper, "MIT Guide to Lock Picking" by an author calling himself Ted the Tool (www.lysator.liu.se/mit-guide/ MITLockGuide.pdf), discusses the vulnerabilities of tumbler locks.

The server room should have the best lock the company can afford. The Department of Defense spending $5000 to $10,000 on a lock where protecting resources might be a life-or-death situation.

For better security, some organizations require using **card access**. With this method, a card is scanned, and access is given to the cardholder while documenting the time of entry. This method also makes it possible for one card to allow access to several doors without having to issue multiple keys or having users memorize different combinations.
